April 18, 2015

The Honorable Susan Rice

Advisor to the President for National Security Affairs

The White House, Washington D.C. 20500

Dear Ms. Rice

I am enclosing the fourth in a series of White Papers that address the issue of Security in the North American Grid. All have been sent to your office over the past 4 years. These reports point to the progressive failure of the industry, its principal regulatory body, the Federal Energy Regulatory Commission, and sector-specific departments to meet their joint responsibilities to protect the Grid, under the Federal Power Act of 2005.

***Today, the Russian FSB and its Chinese counterpart are deep into Grid networks and control systems, doing reconnaissance, installing malware, and preparing these systems for disruption, or worse.*** But our federal authorities, departments and the Congress, stay focused on information sharing or pseudo-privacy issues, ignoring these embedded threats. The White House keeps issuing Executive Orders that simply fail to address the actual threats to the nation, unwilling to empower competent authorities to combat the adversaries within the Grid environment. There is little possibility of the National Security Community (Cyber Command and NSA) being able to blunt an actual attack, ***from a cold start.*** Their restraints must be removed.

The enclosed report documents the industry, FERC, DHS and DOE failures to come to grips with the major flaws of their cybersecurity standards and overstated Grid "resiliency". The paper also realistically documents threats and vulnerabilities. With the growing maturity of cyber capabilities in militant Islamic nations and terrorist groups, it is only a question of time before a serious attack on the Grid occurs. The American public is overdue for a much more balanced treatment of privacy concerns and actual threat issues.

For Critical Infrastructure, this crisis is the major national security issue, hence this letter and enclosure. Loss or serious disruption of the Grid will have enormous adverse effects on national security establishments and civil infrastructures. The recommendations in the enclosure really must be set in train now, if it is not already too late.

Most sincerely

George R. Cotter

George R. Cotter

Enclosure: Security in the North American Grid, A Nation at Risk, April 8, 2015

Distribution:

Chairman, House Committee on Homeland Security

Ranking Member, House Committee on Homeland Security

Chairman, U.S. Senate Committee on Homeland Security & Governmental Affairs

Ranking Member, U.S. Senate Committee on Homeland Security & Governmental Affairs

Chairman, Senate Select Committee on Intelligence

Ranking Member, Senate Select Committee on Intelligence

Chairman, House Permanent Select Committee on Intelligence

Ranking Member, House Permanent Select Committee on Intelligence

Chairman, Senate Energy and Natural Resources Committee

Ranking Member, Senate Energy and Natural Resources Committee

Chairman, House Armed Services Committee

Ranking Member, Senate Armed Services Committee

Assistant to the President for National Security Affairs

Secretary, Department of Homeland Security

Secretary, Department of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics

Chief, National Guard Bureau

Secretary, Department of Energy

Director, National Intelligence

Director, National Security Agency/Commander Cyber Command

Director, National Institute of Science and Technology

Chairman, Federal Energy Regulatory Commission

Chairman, U.S. Nuclear Regulatory Commission

North American Electric Reliability Corporation

# SECURITY IN THE NORTH AMERICAN GRID
# A NATION AT RISK

## A White Paper

George R. Cotter
April 8, 2015
grcotter@comcast.net

## *Disclaimer*

***I take full responsibility for this study. The information is all from the public domain. The interpretations, judgments and comments are mine. It has had no endorsement from any organization and none is intended.***

***George R. Cotter***

***April 8, 2015***

*Security in the North American Grid*

*A Nation at Risk*

## *Outline*

***Security in the North American Grid***

***A Nation at Risk***

***April 8, 2015***

## *I. Background*

For well over forty years, the nation's electric utilities have worked collectively on the interconnection of electric generation and transmission systems with a goal of an integrated and reliable National Grid. Federal deregulation over that period has encouraged many mergers and multistate reliability consortiums, paralleled by favorable tariff rules including development of a wholesale ("day ahead") market. Key enabling legislation, the Federal Power Act of 2005, created an Electric Reliability Organization (ERO) to develop cybersecurity standards for the protection of the Grid. The North American Electric Reliability Corporation, a not-for-profit consortium, was selected to fill the ERO function. For reliability reasons, the industry had organized itself into 8 regions (see map) that have evolved from business, interconnection and reliability forces. Cybersecurity responsibilities naturally parallel these reliability regions. Industry consolidations also tend to follow these boundaries. From the outset, CIP standards largely addressed cybersecurity issues of this increasingly integrated array of regional electric utilities--- generation, transmission and (some) distribution facilities. The cyber assets and their associated control facilities exist for both management of the Grid and ensuring its technical integration.


NERC-developed critical infrastructure protection (CIP) standards require approval by the Federal Energy Regulatory Commission. The initial FERC Order No. 706 in 2008 started the formal process of approval of CIP standards; essentially building on voluntary CIP standards created by NERC a few years earlier. CIP Version 3 standards are currently in effect across the industry. ***CIP v3 standards apply to utility generation and transmission assets and only indirectly to associated cyber assets***. There has been continuing iteration between NERC and FERC to replace CIP v3 standards with a more applicable set, initially v4. The CIP v4 set, while an improvement over v3, provided such limited coverage that they were not implemented and were overtaken by CIP v5 standards, approved with

qualifications by FERC.[1] The CIP v5 standards will not replace v3 for several years and are, in fact, subject to some further revision and approval by FERC.

In recent years, concerns on other aspects of "Security of the North American Grid" have arisen; notably Physical Security and more generally, Energy Security (the latter defined as assurance of the supply of energy to meet national needs). This White Paper will address several of these issues as they relate to cybersecurity.

## *II. Introduction*

This White Paper is the fourth[2] in a series that examines technical and policy issues of cybersecurity protection for the North American Grid. They have been sent to policy-makers and federal institutions that share responsibility and/or authority for homeland defense. The fundamental issues that are dealt with here are industry assertions that **resiliency** of the Grid coupled to a **standards-only** implementation of security protections is sufficient to ensure availability of electric power to civil and national security institutions in the face of known threats, widespread vulnerabilities, and in the absence of a grid-wide operational cybersecurity system.

Prior papers in this series have addressed administration steps to bolster CIP activities within existing authorities, and congressional actions to legislate information sharing. Recent administration actions centered on an Executive Order have not resulted in any significant changes in critical infrastructure protection in the energy sector. Congressional bills have failed to clear both houses of Congress and major legal issues of liability protection, information sharing, constitutional privacy and civil rights and several deficiencies of the FPA, remain to be resolved by legislation underway and follow-on White House Executive Orders.

The industry's level of protection has remained stalled over the past several years, hung up on an unworkable set of standards (v3) and a constantly-evolving set of draft standards. The composition (i.e., hardness) of the standards and the process of compliance have also been unclear. The lack of an integrated, Grid-wide, 24/7 operational cybersecurity program alone raises serious doubts about the security of the North American Grid since the standards apply primarily to individual utilities, i.e., sites[3] and as will be discussed in this paper, revealing a near-total lack of cybersecurity in the communications and network fabric that links these sites together. The law excludes all Grid distribution networks

---

[1] FERC Order No. 791, "Version 5 Critical Infrastructure Protection Reliability Standards", November 23, 2013

[2] "Security in the North American Grid", 18 September 2011, "Security in the North American Grid – An Update" March 31, 2012, and "Security in the North American Grid – 2nd Update" May 31, 2013.

[3] Nuclear sites operate under separate Nuclear Regulatory Commission Rules and Regulations for Cybersecurity.

(largely urban areas, Alaska and Hawaii)[4] thus electric service to major segments of society depends solely on the resiliency of the BES. ***Therefore most electric distribution systems for major centers of society, major metropolitan areas, major military installations can be attacked with impunity and taken down; the "resiliency" of the BES notwithstanding.*** Note also that the activities of 16 regional and sub-regional Reliabilty Authorities, as well as NERC itself, responsible for operational reliability of the Grid are not bound by CIP standards and appear to be immune from all but legal actions relative to maintenance of Security in the National Grid.[5] Audit and compliance functions under CIP standards are largely decentralized to NERC regional authorities and are largely paper (table top) reviews.

***Comment: With the near-completion of CIP v5, NERC, and FERC essentially assure the nation that the presumed resiliency of the Grid coupled to this set of cybersecurity standards is sufficient for the Grid to survive and recover from a cyber attack without an extended nation-wide or major regional power loss; i.e., a crisis that would seriously damage the nation's national security, industrial, financial, health and social infrastructures..***

***Even to imply survivability of the Grid, the industry, NERC and FERC must explain how this is possible, given:***

***1. The hundreds of thousands of Grid ICS devices exposed to penetration through direct Internet access.***

***2. The near-total absence of encryption protection for the communications and network systems between the Grid's ICS devices and SCADA systems, and control centers.***

***3. The absence of an operational Grid-wide 24/7 cybersecurity monitoring effort.***

***4. Therefore, the complete absence of Grid situational awareness or a Grid-wide recovery strategy in the event of a major attack.***

***5. And therefore putting at risk critical off-site AC power distribution to over 50 nuclear generation sites; risking nuclear contributions to the Grid (at best) and nuclear devastation (at worse).***

## *III. CIP V5 Standards*

### *A. Development Chronology for CIP v5 Standards*

[4] By law, such distribution assets are not included in the standards process unless linked into a transmission asset covered by CIP v5.

[5] Individual firms and not-for-profit consortiums backing up these authorities are, or course, subject to the CIP standards.

CIP v4 was filed with FERC on February 19, 2011 and was approved by FERC[6] but not implemented. CIP V5 was first posted by NERC for 45 day comment on November 7, 2011, went through a final comment phase, was subsequently approved by the NERC Board of Trustees and filed with FERC on 31 January 2013. FERC's final approval of CIP v5 (with qualifications) occurred on November 22, 2013.[7]

The NERC process basically follows the IEEE ANSI model, is largely transparent and carefully recorded. A Standards Development Team ((SDT) of approximately 8 members is created with several members from NERC Staff but mostly from industry. The SDT has the benefit of voluminous comments on prior CIP versions, specific directions from FERC as well as carry-over issues not resolved in previous iterations with FERC. There are at least two separate 45 day comment periods, open to industry members, industry associations, NERC regional entities and the public. Very few public comments are received, however.

An SDT ballot is taken following the final comment period. Votes are registered on CIP Standards, Requirements and Compliance features, guidance on each standard and an Implementation Plan, Violation Risk Factors and Violation Severity Levels. A detailed record of these stages accompanies the NERC formal proposal to FERC. The FERC Docket is also open to comments from the industry, NERC and the public. Here also, few public comments are received. The result:

**CIP V5 Standards**

| CIP | Title | Definition |
|---|---|---|
| 002-5 | BES Cyber System Categorization | Low, Medium, High |
| 003-5 | Security Management Controls | Cybersecurity policies |
| 004-5 | Personnel and Training | Security awareness, risk assessment, access management |
| 005-5 | Electronic Security Perimeter(s) | Discrete Electronic Access Points |
| 006-5 | Physical Security BES Cyber Sys. | Physical security plan |
| 007-5 | Systems Security Management | Technical, operational and procedural steps |
| 008-5 | Incident Reporting, Response | Incident reporting -1 hour of recognition |
| 009-5 | Recovery Plans BES Cyber System | Response for stability, operability, reliability |
| 010-1 | Configuration Change Management | Monitoring, vulnerability assessment |
| 011–1 | Information Protection | Consolidation of information protection requirements |

[6] FERC Order No. 761 "Version 4 Critical Infrastructure Protection Reliability Standards", Docket RM11-11-000, April 19, 2012.
[7] FERC Order No. 791 op. cit.

## B. Characterization of CIP v5 Standards

The Standards development process is enormously influenced by industry; clearly Congressional intent in the FPA. Final ballots on CIP Standards regularly show an approval rating in the high 80%. The CIP v5 Implementation plan calls for final implementation for High and Medium Impact Cyber Assets two years after notice in the Federal Register. High Impact cyber assets apply to large control centers. Medium Impact cyber assets cover generation and transmission systems and control centers not included in High Impact category. Note the industry will have three years for implementation of CIP v5 standards for Low Impact Cyber Assets.

Despite the huge investment by the industry in the creation of these standards, there is no escaping the fact that it reflects, almost totally, a process-driven architecture. This can be seen in the character of the 10 basic standards in the foregoing table. There is a total of 36 "Requirements" that are mandatory across these 10 basic standards. A careful dissection of these requirements reveals the nearly complete absence of technical metrics, technical system examples, specification minimums; indeed, anything that would support "benchmarking" of a utility in any audit or compliance examination.

`The industry structure for use of these standards is the nation-wide collection of nearly 2000 utilities, each responsible for implementation at generation, transmission (and some distribution) facilities. One would therefore expect heavy emphasis on "process" to ensure conformity to these standards. But there can be no consistency in their application to operational facilities in the near-total absence of hard technical criteria. In one case of access controls, the SDT struggled with language to define technical controls but in the face of industry resistance, talked themselves out of any technical specifications. It is left to auditors and compliance reviewers, therefore, to understand each utility's technical approach to access controls.

Is there an alternative to the NERC-developed CIP standards? Yes, both the law and FERC Order No. 706 urged NERC to consider the NIST standards that have overwhelming acceptance across the federal government, much of industry, and the Nuclear Regulatory Commission. NERC has alternately claimed "similarity" to NIST Standards or has defined its tasks as being quite unlike the users of NIST standards. NIST standards avoid inclusion of specific industry products or systems while at the same time providing sufficient technical detail that users can readily implement the standards in their competitive procurement environments. The NIST flagship publication, SP 800-53v4 has an annex of over 100 pages describing technical specifications for cybersecurity controls. In resisting adoption of NIST cybersecurity standards, the industry represented by NERC reveals unwillingness to accept the discipline and technical rigor adopted by users of the NIST standards.

## C. Additional CIP v5 Issues

1. NERC's strategy for CIP v5 development is the assertion that coverage of Medium and High Impact cyber assets is sufficient given the claimed resiliency of the Grid. However, the majority of cyber assets fall into the Low Impact category where standards have little effect. This has troubled FERC throughout the CIP standards process. In the sophisticated world of

information operations, this claim is simply unsubstantiated; it presupposes application of standards to Medium and High Impact cyber assets will offset zero-day incursions. It fails to appreciate that sophisticated attacks involve oblique vectors, many such attacks will seek the path of least resistance; i.e., through Low Impact assets, and across a totally vulnerable network. ***Russian presence in Grid networks with malware largely undefined by a consortium of excellent security firms illustrates this point.*** The weak technical standards on mobile devices, passwords, access controls, etc., will simply make matters worse.

2. Mapping of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems by network tools (SHODAN for example) reveal hundreds of thousands such devices directly facing the Internet (i.e., accessible).[8] These devices are endemic to the Grid being the backbone of digital control of switches, transformers, and other utility systems. CIP standards development has completely avoided these most vulnerable targets. Apparently FERC and NERC have relegated this massive vulnerability to the "too hard" pile.

3. CIP 002-5 Standard lists four areas that are exempt from classification as cyber assets. These are:

    a. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

    b. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

    c. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cybersecurity plan pursuant to 10 C.F.R.Section 73.54.

    d. For Distribution Providers, systems and equipment that are not linked into certain functions included in CIP 002-5 Transmission systems.

Items a, c and d in (3) above are obvious jurisdictional or legal boundary conditions. Item 3b, however, is an exemption integral to CIP v5 standards; indeed it represents a stake in the ground absolutely excluding from the standards, communications and network systems that are the backbone of the Grid. The ostensible reason given for this exception is that the industry does not "own" the carrier systems these networks ride on. FERC has been reminded on numerous occasions that Grid-wide communications and network security challenges parallel those used by all major organizations. FERC's task cited below shows FERC's unease with its multi-year failure to meet the explicit operational communications and network security requirements of the law. However, FERC failed to challenge this exception in approving CIP v5 standards and will (again) have to address this inconsistency with the NERC response to Order No. 791, which was due February 13, 2015 but does not yet appear to have been filed.

[8] See Section VIII, Vulnerabilities in this paper for a graphic two-year view of ICS internet accesses revealed by the Shodan mapper.

*Comment: While the formal regulatory exchanges between NERC and FERC are in the public domain, there is almost no media comment on the major issues; indeed, the arcane energy business largely discourages detailed media attention. For this reason, this paper goes to considerable lengths to explicitly cite FERC tasks and NERC responses to enable the reader to better understand the outstanding issues of FERC Order No. 791, as they affect the nation.*

In its Order No. 791 FERC approved CIP v5 standards ***("as an improvement over CIP v3")*** but with a number of qualifications, cited below. Several additional issues trace back to concerns expressed in its original Order No. 706 of 2008, but under industry pressure, have been delayed "for further study".[9] What follows are extracts from FERC Order No. 791 along with final NERC responses from its Standards Development Team, as approved by ballot of NERC stakeholders on 2 February 2015 and the NERC Board of Trustees on 12 February 2015

The four principal tasks of Order No. 791 were:

> **"1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements.**
>
> **2. Develop modifications to the CIP standards to address security controls for Low Impact assets.**
>
> **3. Develop requirements that protect transient electronic devices.**
>
> **4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks."**

FERC's Order gave NERC a year to provide recommended changes or modifications to V5 Standards. The Order also required NERC to make "informational filings" on several other issues identified below

- ***Definition of Communications Networks***

**FERC:** ***"We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. (Emphasis added) The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication***

[9] Extract from FERC Order No. 791. **"Accordingly, we decline to direct any modifications to the CIP Reliability Standards at this time to address the NOPR concerns regarding communications security, remote access, and the NIST Risk Management Framework. Rather, we agree with NERC and a number of commenters that suggest a technical conference discussing these issues as an appropriate next step."**

*networks." The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule."*

**NERC:** *"The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for nonprogrammable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset."*

*"The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards."*

*Comment: NERC is in defiance of the order in failure to (1) create a definition of communications networks and (2) to develop new or modified Reliability Standards to address protection of the Grid. NERC cannot limit this task to Physical Security of site hardware components as they attempt to do in their response to Order No. 791. For over 9 years, NERC has been kicking this can down the road and in the absence of any remand on CIP orders from FERC, imperils the nation with an unsecured Grid network fabric. There can be no misunderstanding the intent of Congress, the security of communications networks is paramount. While the FPA was generally focused on standards in 2005, their intent clearly included operation of secured communications networks as well, as seen from the following extracts:*

*FPA Section 215 (a) Definitions, Para (3) explains that reliability standard means a requirement approved by the Commission under this section, to provide for reliable operation of the bulk power system. The term includes requirements for the operation of existing bulk power system facilities, including cybersecurity protection (Emphasis added).*

*FPA Section 215 (a) Definitions, Para (4) indicates: "The term reliable operation means the elements of the bulk power system.....(resulting in) cascading failures...including a cybersecurity incident....." (Emphasis added)*

*FPA Section 215 (a) Definitions, Para (8) defines "cybersecurity incident" as "a malicious act or suspicious event that disrupts or was an attempt to disrupt the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system." (Emphasis added.).*

*Comment Continued: Further, NERC's effort to characterize the modern networks used to link Grid utility and regional generation, transmission and distribution facilities into a National Grid as "nonprogrammable" is a deliberate effort to conflate the FPA's distinction between site "programmable electronic devices" and "communications networks". Modern networks are characterized by switches, routers, and modems that are inherently digital and programmable. NERC's equally nonsensical excuse that the industry does not "own" the communications fabric is immaterial; few if any national networks (DoD, State, NASA, etc.) own the carrier systems that their networks employ. Congress is not legislating NERC and FERC responsibility for securing carrier systems, only the operational networks that ride on those systems*

- **Ambiguity and Enforceability of "Identify, assess, and correct" Language**

1. ***Low Impact Assets.***

**FERC:** ***"For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d) (5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements. Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns regarding the "identify, assess, and correct" language. The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule."***

**NERC:** ***"The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1."***

***"The SDT revised Requirements R1 and R2 of CIP-003-6 7 to include additional specificity regarding the processes that responsible entities must have for low impact BES Cyber Systems. In addition, the SDT developed objective criteria type and routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category."***

***"To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and***

*Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility-site level."*

*"The SDT confined these revisions in CIP-003-5, Requirements R1 and R2 to the following areas:*

*a. Cyber Security Policy: R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan.*

*b. Cyber Security Plan(s): R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s)."*

*Comment. Note again, the emphasis on "policy" and "plans" rather than hard technical detail. The cyber security plan must cover the 4 areas as specified in Attachment 1 of CIP-003-5 i.e., Cyber Security Awareness, Physical Security Controls , Electronic Access Controls, Cyber Security Incident Response (details omitted). These changes simply extend the same technically-deficient standards to the otherwise unbounded low impact cyber assets. Will FERC accept these modifications to CIP v5? Given the exclusions granted NERC and the industry in accounting for Low Impact Cyber Assets, how would FERC be assured that application of these standards and requirements was consistently applied in the myriad of audits and compliance certifications occurring across the entire set of 2000 Grid entities. Further, the SDT's "LERC" and "LEAP" definitions are transparent attempts to ensure that Low Impact Assets involving communications and network facilities are essentially limited to PSPs; i.e., do not apply to Grid-wide systems.*

### 2. Categorization of Cyber Assets

**FERC:** *"The Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets."*

**NERC;** *"Based on comments and feedback from the draft proposed. Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing"*

*Comment: One of the major difficulties with the CIP v4 proposed standards was the large percentage of assets that would be outside the "Brightline" definition for low risk assets. At that time, FERC was concerned over the cumulative vulnerability effect on Grid Reliability for low risk assets. The directed informational filing shows FERC concern that these lengthy exchanges on low impact cyber assets have not resolved the issue that brought CIP v4 to its knees. For CIP v5, low impact assets remain undefined, the category contains all cyber assets not covered by the metrics of Medium Impact and High Impact cyber assets. Thus, almost ten years after the passage of the FPA of 2005, there is still no definitive tabulation of "low impact" cyber assets pending the completion of the informational filling called for in the FERC task. The "cumulative effect of an unknown number of low impact assets remains a major security concern.*

FERC had additional concerns over transient electronic devices as shown in the following extract from Order No. 791 (some of which will undoubtedly qualify as "low impact" cyber assets): **"We direct NERC, pursuant to section 215(d)(5) of the FPA, to develop requirements that protect transient electronic devices (e.g., thumb drives and laptop computers) that fall outside of the BES Cyber Asset definition. While we are persuaded by NERC and others that it would be burdensome to include transient devices as BES Cyber Assets, we also believe that further protections are needed in light of the potential vulnerabilities associated with transient devices."** It is not clear what NERC authorities are for the protection of cyber assets falling outside BES Cyber standards. It may remain for FERC to develop alternative methods for their protection.

## D. NERC Board of Trustees Approval

On 11 February, 2015 the NERC Board of Trustees approved the CIP v5 modifications as discussed above, including CIP 014-1 Physical Security Standards (see below).. A NERC filing with FERC should have followed. Policy comments to the NERC BOT were extensive with expressions of concern on resources required, complexity of the CIP v5 Transition Plan, ambiguity of much of the requirements language, with concerns over compliance and audit variability across the NERC Regions. Respondents expressed need for precision on NERC's guidance on Physical Security Standards.[10]

[10] NERC Members Representatives Committee (MRC) Memorandum to NERC Board of Trustees, Feb 5 2015

*Comment: What are some of the missing, critical cybersecurity components of the Grid, elements that would be required in any Grid-wide Operational Cybersecurity Program?*

- *Modeling and Simulation, Local, Regional, Grid-wide*
- *Encryption, Key Management, Digital Signatures*
- *Security Incidence & Event Management (SIEM); Local, Regional*
- *SCADA, ICS, PLCs-Device Identification and Verification, Control Center Automation*
- *Supply Chain Management; across the Critical Cyber Infrastructure*
- *Controlled Interfaces, Access Port Limitations, Split Tunneling*
- *Vulnerability Assessments, Monitoring, Scanning, Covert Channel Analysis*
- *Centralized Situational Awareness, System of Alerts, Advisories, Directives*
- *Minimal Threat Signature Guards (e.g., Einstein 3)*
- *Network and Communications Protection; Local, Regional, Grid-wide (e.g., US-Canada)*

*After Five Iterations, Mostly Process, Form; Near Absence of Deep Technical Standards, What are the Fundamentals of CIP Security Policy for the National Grid? After a Decade, Why is there still No Regional or Grid-wide Operational 24/7 Cybersecurity Program? (Note: The foregoing summary was presented to several of the FERC Commissioners in November 2014 by the author of this paper participating in a vulnerability brief.)*

## *IV. Related Security Issues*

There are a number of regulatory actions that affect the availability of electric power and that complicate CIP issues. Two are discussed below; Physical Security of energy facilities and the effect of solar flares on major Grid installations, including their cyber assets.

### *A. Physical Security*

On April 13, 2013 transmission and communications facilities at the PG&E Metcalf substation in San Jose, CA were attacked. Significant damage to 17 transformers occurred, surgically holed to permit cooling oil to escape but delaying or avoiding a blaze in the facility. The perpetrators entered a manhole and cut two fiber optic cable prior to the transformer attack, indicating their knowledge of this type of facility and the importance of blindsiding the control center.[11] They were apparently unaware of a backup radio link or chose to ignore it.

[11] Cutting the fiber optic cables constituted a cyber attack. Note CIP 003-5 levies requirements for physical security of cyber assets.

The perpetrators have not yet been apprehended. PG&E initially characterized the event as vandalism; however the FBI was called in. Subsequently, NERC and FERC organized a US tour to brief major utilities. Very likely for sensitivity reasons, the event was low-keyed. However, following a report in national media early in 2014, an exchange of letter between US Senate leadership and FERC occurred with the Senate raising questions of the need for physical security standards.[12] FERC initially resisted, stating that education, not standards were the appropriate response to the incident. Nonetheless, FERC shortly tasked NERC to develop a minimum set of standards, only focused on high value transmission facilities and related control centers.


**Shots in the Dark**

A look at the April 16 attack on PG&E's Metcalf Transmission Substation

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| **12:58 a.m., 1:07 a.m.** Attackers cut telephone cables | **1:31 a.m.** Attackers open fire on substation | **1:41 a.m.** First 911 call from power plant operator | **1:45 a.m.** Transformers all over the substation start crashing | **1:50 a.m.** Attack ends and gunmen leave | **1:51 a.m.** Police arrive but can't enter the locked substation | **3:15 a.m.** Utility electrician arrives |

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)
The Wall Street Journal

For several years, NERC had a SDT developing physical security standards for the Grid. Additionally, CIP v5 Standards includes a standard for physical protection of cyber assets (CIP 003-5), it being generally accepted that cybersecurity is incomplete without reasonable safeguards to physically protect the asset, (similar to standards addressing personnel security for cyber assets). Within three weeks of the Metcalf attack, all records of NERC development of Physical Standards was removed from public access. The assumption in this paper is that NERC did this to avoid liability issues that might arise.

The Physical Security order was one of the most rapid standards development cycles ever,[13] it sets a very high bar for applicability, essentially only transmission and related control systems covered by Medium Impact cyber standards for Transmission Systems. There are six requirements owners and operators of such systems must satisfy:

R1 - Periodic Risk Assessments of stations and substations which, if lost, would lead to instability of the BES, and identify primary control stations.

---

[12] US Senate Letter to FERC Signed by Senators Reid, Franken, Wyden, Feinstein, dated 7 Feb 2014 and FERC Response Dated 11 Feb 2014

[13] On November 20, 2014, FERC issued Order No. 802 Physical Security Standards. It becomes CIP 014-1 in the NERC CIP feature set.

R2 – An unaffiliated professional third party must verify the foregoing risk assessments.

R3 - Operators of control systems would have to be notified of the identification of facilities coming under R1.

R4 – Each owner/operator must evaluate the potential threats and vulnerabilities of physical attack.

R5 – Each owner/operator must develop and implement documented physical security plans.

R6 – An unaffiliated third party must review the evaluation in R4 and the plan in R5.

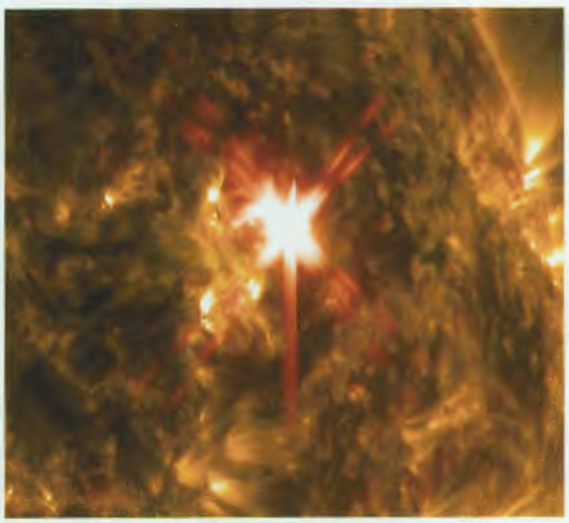
In its Notice of Proposed Regulation (NOPR) on Physical Security, FERC had proposed to permit appropriate federal authorities, including the commission, to add or remove facilities from compliance with the final standard. It also stated a requirement for an informational filing by NERC on a need for a consistent policy for High Impact Control Centers and an informational filing requiring NERC to show the effect on resiliency of the BES with the loss of a major transmission facility. ***In the final order, No. 802, FERC dropped the requirement for additions or removals by appropriate federal authorities, under considerable pressure from NERC and the industry.*** While it retained the requirement for an informational filing on high impact control center "consistency", it extended the period of response to two years. And it dropped the requirement for demonstration of resiliency. It reaffirmed the requirement for unaffiliated review by third parties, reaffirmed the exclusion of generators from the Order, and reinforced a strong requirement for NERC's implementation on sensitivity of data requiring protection from public revelation.

***Comment: The Metcalf attack was a signature moment for the industry, a realization of how exposed they are and how, over the years of their creation, there has been little attention to their physical protection. It is a monumental challenge for the industry, and the nation, to address physical protection at this late date. However, it is certainly appropriate for FERC to worry about physical protection of those facilities most critical to the resiliency of the BES.***

***Many inconsistencies in security protection of the National Grid arise as a result of the crash effort to install Physical Security standards. For example, there are major high impact control stations included in CIP 002-5 that will not be covered by physical standards because of falling below the cutoff in metrics defining transmission stations, substations and associated control stations. The complete absence of generators cannot be explained away simply because standards for transmission systems theoretically assure the resiliency of the Grid. Many Reliability Coordinators will be blindsided on a physical attack; yet have unique regional responsibility for maintaining the reliability of the Grid. Further, FERC and NERC exclude any steps utilities must take to minimum protection of facilities; leaving it to utilities and compliance officials to determine. Is this any more difficult that the steps the NRC has taken over the years to ensure the protection of nuclear facilities? At a minimum, the NRC 'layers of protection' model could have been copied by FERC and NERC.***

***Comment Continued: But perhaps the most serious difficulty with FERC's Order No. 802 lies in its conviction that maintaining the resiliency of the Grid satisfies it obligation for protection of the public, its civil social and economic structures and its national security needs. The loss, for example of a single electric facility could create an unrecoverable loss to a major national security activity; one that must survive indefinitely for protection of the nation. It is unreasonable to expect such organizations or facilities, totally dependent on the Grid, to accept the minimalist Order No. 802 physical security "standards" arising out of the Metcalf attack. A far more practical solution would in fact, leave options for critical civil and national security installations to be identified, validated as to the criticality of their survival, and be included in any process for identification of electric facilities requiring enhanced physical security.***

## *B. Solar Storm Effects*



There is disagreement between the industry and major segments of the scientific community on the effects of geo-magnetically-induced current (GIC) on the Grid. These effects are created by high energy solar flares whose ion flows impact the earth's geomagnetic field. NERC was tasked with developing one or more reliability standards[14] to address GMD events, a requirement that arose out of an Oak Ridge National Laboratory study of GMD's that had been requested by FERC. That study seriously questioned the estimated strength of the benchmark GMD, a 1-in-100 year Carrington event, of 1859, used by NERC in its response to the FERC Order.

On June 19, 2014, FERC approved Phase 1[15] of a GMD standard that required owners and operators of the Bulk-Power System to develop and implement operational procedures to mitigate the effects of GMDs consistent with the reliable operation of the Bulk-Power System.

In the second stage, the Commission directed NERC to submit, within 18 months, one or more Reliability Standards that requires owners and operators of the Bulk-Power System to identify and assess benchmark GMD events that would require a protection plan considering operational procedures and training, but also potential impacts from age, condition, technical specifications, system configurations or locations. These strategies could include automatically blocking GICs from entering the BPS.

---

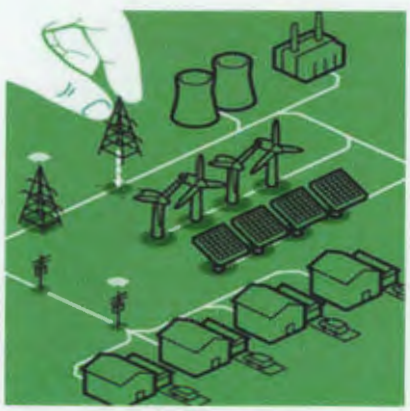
[14] FERC Order No. 779 Docket No. RM14-1-000

[15] FERC Order No. 779 op.cit.

The controversy arises because the evaluation of Benchmark Events will use NERC GIC standards that competent authorities assess as being too low by a factor of 2 to 5, fail to take into account locational variances (latitude anomalies), were extrapolated from a narrow set of observations from Finland taken during non-significant events, fail to use US and Canadian observations during three events that exceeded the Carrington event.[16] These issues were well-known to NERC during the SDT run-up, since a number of studies of solar flares and their actual effect on Grid installations were represented by knowledgeable individuals and organizations concerned over the NERC/FERC staged minimalist construct for the "Reliability Standard". The record shows that the SDT watered down the draft standard until it could get a consensus vote through the SDT. This culminated in the narrow Phase 1 rule that limited responsibility for management of a major GMD event to procedural steps, with little direction from FERC to compel scientific objectivity for Phase 2.

**Comment: There is an old saw "Don't ask the question if you ae not going to like the answer." FERC certainly fell victim to it when it read the Oak Ridge study it had ordered. FERC was aware of numerous studies and papers that challenged the SDT response to Order No. 779. This final order deliberately sidestepped all major issues, scientific-based facts, and potential risks to major regions of the country. FERC's pious declaration that the Reliability Standard "is just, reasonable, not unduly discriminatory or preferential, and in the public interest" constituted abject subservience to NERC and the industry. If FERC were truly interested in the public interest, there were many options available for a balanced evaluation of GMD evidence, current and future, with interim protections to minimize damage to the Grid until an honest risk/cost assessment, impacting industry, was available. Accumulated PMU data (see following section) would be invaluable to such an effort. The risks to the Nation are, of course, compounded when nation/state adversaries or domestic activists develop strategies to test malware under the cover of a GMD event. Clearly, FERC, NERC and the industry are simply planning to "tough-it-out" through the current high sun spot cycle.**

## *V. Grid Modernization*



An important question is whether cybersecurity will be a significant component of industry efforts to modernize the Grid. Most security professionals understand the importance of "baking" security into new developments; it is always more difficult to add security later. Initiatives such as the development of programmable inverters in solar systems discussed below create new vulnerabilities and their introduction should include appropriate

[16] For an incisive examination of these factors, see comments of John Kapperman and Curtis Birnback on Draft Standard TPL-007-1, submitted to NERC on October 10, 2014.

safeguards against their subversion by hactivists or the nation's adversaries.

## A. Solar Inverters

There are predictions of significant increases of solar power based on steady reduction in cost and increased efficiency of solar panels. Recent developments in Germany[17] and in California identify an added function for Solar, beyond contributing power to the Grid. Advances in smart inverters now permit Solar systems to help in a "balancing" role, as reactive power sources do in the nation-wide Grid. California's smart inverters will, like Germany's, counterbalance solar's direct impact on grid voltage. But they will also dynamically regulate voltage. If a smart inverter detects voltage exceeding 1 percent of normal, it will absorb additional reactive power. And if line voltage drops below normal—as can occur when passing clouds suddenly squelch photovoltaic power—the smart inverters will bolster it by injecting reactive power. Efforts are under way to incorporate California's upgrades into the IEEE 1547 standard governing distributed power devices, which would accelerate smart-inverter use across the United States. At present in California, this affects only locally-distributed power; however with strong efforts in many states to accelerate clean energy initiatives, the smart inverter technology should spread rapidly to other regions.[18] Grid-wide dependencies on solar assets is likely to remain low for many years; however if they remain vulnerable to malware, there could be significant local blackouts. Obviously, security measures should increase proportional to the increase in solar dependencies.

## B. North American SynchroPhasor Initiative (NASPI)

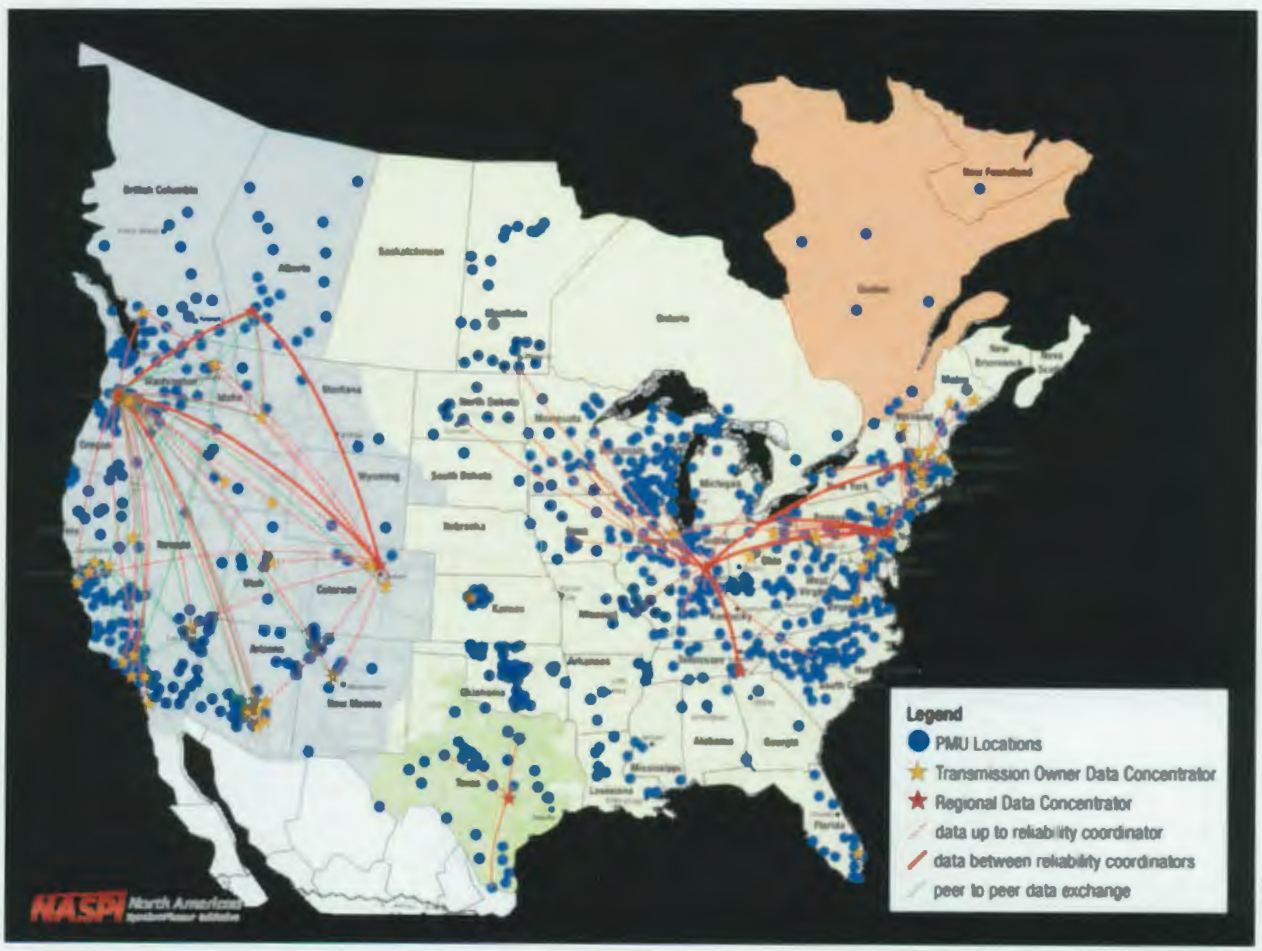
Over the past several years there has been extensive introduction of systems to automate critical control functions in transmission systems, e.g., "synchrophasor" technologies. A synchrophasor is a time-synchronized measurement of a quantity described by a phasor. Like a vector, a phasor has magnitude and phase information. Devices called phasor measurement units (PMUs) measure frequency and voltage. These measurements allow operators to calculate parameters such as frequency and phase angle. PMU measurements are time-stamped to an accuracy of a microsecond, synchronized using the timing signal available from global positioning system (GPS) satellites or other equivalent time sources. Measurements taken by PMUs in different locations can be accurately synchronized with each other and can be time-aligned, providing the relative phase angles (of 60 cycle frequencies) and voltages between different points in the system as directly-measured quantities. Synchrophasor measurements can thus be combined to provide a precise and comprehensive "view" of an entire interconnection. This is probably the most significant development permitting the industry to reliably balance power transmissions across the geographically-dispersed Grid.

The Recovery and Reinvestment Act of 2009 matched by private industry funds has led to the installation of PMUs in over 1700 installations (see map below). The DOE and industry investments also funded installation of high-speed synchrophasor data networks, development of technology

[17] IEEE Spectrum, "How Rooftop Solar can Stabilize the Grid", 21 January 2015.

[18] Note there are strong industry efforts in a number of states lobbying for a tax on solar power inserted in the Grid on the basis that solar must pay its fair share of the costs of transmission and distribution resources. Clean energy advocates are strongly resisting this tax.

interoperability standards for PMU measurement, functionality and data formats. At the same time, DOE funded a variety of R&D projects to develop advanced synchrophasor data applications and analysis tools. The network of PMUs enable grid operators to theoretically observe the bulk power system across an entire interconnection, understand grid conditions in real time, and diagnose and react to emerging problems. But note how many PMU's on the map below are not yet network-connected. PMUs substantially automate the data that operators routinely see from SCADA and EMS systems. Relatedly, forensics on malware seen on Grid networks reveal adversaries' focus on human-machine operator interfaces (HMI's).[19]




[19] US CERT ICS Alert-114-281-01A, November 3, 2014

## C. *Eastern Interconnect Data Sharing Network (EIDSN)*


For some time, NERC has used a dedicated network (NERCnet) for communications with its 16 Reliability Coordinators (RCs) and Independent System Operators (ISOs). NERCnet, a point-to-point or "Frame" configuration, has accommodated the flow of facility status data between "Responsible Entities" to assist in maintaining reliability of the Grid. However, NERC reportedly has had considerable difficulty in allocating funding for this and has absorbed some costs in the NERC budget. A series of mergers and funding issues with carrier vendors has resulted in NERCnet being on a month-to-month contract extension due to expire on 30 June 2015. NERC has been anxious to shift the burden of reliability data flow to industry and several years ago, NERC made the decision to divest the RCs from NERCnet. The Eastern Interconnect authorities started work on creating its own secure coordination network (labeled EIDSN), organizing, in January 2014, a not-for-profit corporation to manage the network. The consortium plans to bill costs separately to each of the network nodes. Four of the 16 RCs (WECC[20] and Western Canada) are not included in this consortium plus Texas. The objective is a two-network configuration to accommodate the current data flow, a decades-old Intercontrol Center Communications Protocol (ICCP) and the growing and more real-time PMU data flows with a "redundancy" network for reliability purposes. The preferred solution is use of MPLS (Multi-Protocol Label Switching) virtual private network (VPN). The EIDSN is experiencing some difficulty in getting this all under contract, establishing secure network connectivity at each of the RCs, and achieving some period of parallel operations with NERCnet for transition purposes. This will ultimately permit much more precise technical phasing of transmission facilities of the Eastern Interconnect across Reliability Regions. The process will ultimately require substantial additional automation to permit more timely, integrated and more automated reaction to anomalous conditions. ***What remains very uncertain is whether the RCs will try to extend secure networking down through the mesh of "Responsible Entities" and critical installations to enhance Grid security.***

***Comment: The Synchrophasor developments described above represent a truly significant advance in the technical integration of regional transmission resources and therefore the reliability of the North American Grid, except of course, for the absence of an overarching cybersecurity architecture including Grid-wide encryption. NERC's divestiture actions certainly enforce the NERC/FERC policy of avoiding involvement in operational Grid matters and of course, divestiture covers NERC's CIP position on restricting communications and network security to cyber assets within site security perimeters only.***

***The SynchroPhasor/PMU initiatives across the Grid should have included a network and communications encryption strategy given the well-established vulnerabilities of ICS, documented by IC Cert and many other authorities. While some organizations are securing this data, DOE should not have left the decision on encryption of data flows to individual utilities, particularly with some Federal funding.***

[20] The Western Interconnect has made substantial progress on dedicated networks for flow of PMU data.

***Comment Continued: It might also be noted that PMU data (with its precise time stamps) would permit extremely -effective warning of the effect of severe solar storms on the Grid, nationally, regionally and locally. Again, one must wonder why FERC (and NERC) completely ignored this potential in its currently open Order No. 779; indeed, existing PMU data during recent solar storms would very likely help resolve scientific debate on GMD effects on Grid. It would also contribute to warning of a cybersecurity attack.***

***A great deal of technical work lies ahead of the industry on the use of advanced instrumentation (and PMU data) to automate Grid management. The 24/7 instantaneous availability of precise instrumentation (PMU) data will almost certainly force FERC to major revisions of their Wholesale ("day ahead") Market pricing strategy. The opportunities for "gaming" the current tariff system are limitless.***

## *Vi. National Organizations; Current Status; Prospects for Change*

### *A. The White House*

Much of the optimism of Presidential Executive Order 13686 of February 13 2013 has faded. Expected outgoing actions by Federal Agencies have not occurred. NIST did in fact complete its Framework for Cyber Security[21] but little follow-up by Federal agencies has ensued, i.e., there is no indication that industry members at any scale have invoked the risk-based analysis of the model. However, a useful feature of the Framework is the inclusion of a direct link to NIST SP 800-53 v4 which has a far more comprehensive set of cybersecurity controls that utilities could use in establishing site cybersecurity systems and procedures. Occasional references to this NIST publication are encouraging. The NIST Framework is totally ignored in any cybersecurity contest by NERC, and for that matter, by FERC (specifically excluded from Order No. 791) despite the fact that both institutions as federally-chartered organizations are theoretically bound by Executive Orders.

On 12 February 2015 in a major policy speech at Stanford University, the President signed a new Executive Order – Promoting Private Sector Cybersecurity Information Sharing.[22] The Order creates the concept of Information Sharing and Analysis Organizations (ISAOs), based on ***"sector, sub-sector, region or any other affinity, including in response to emerging threats or vulnerabilities."*** The order tasks the Secretary, DHS to coordinate the ISAO program. This Order further tasks the Secretary, DHS with the creation of a non-government Standards Organization (SO) to identify a voluntary set of standards or guidelines for use by ISAOs functioning under this order.[23] The Secretary will determine the eligibility of

[21]President's Executive Order, "Promoting Private Sector Cybersecurity Information Sharing", 12 Feb 2015
[22]President's Executive Order, 12 February 2015 op.cit.
[23]The SO standards will be voluntary but the potential exists for conflict with NERC and NRC Critical Infrastructure Standards.

ISAOs for clearances[24]. The NISP EO Manual is substantially amended to empower the Secretary DHS with authority over classified information sharing with ISAOs, with due deference to the authorities of the Secretary of Defense and the Director National Intelligence for classified programs.

A subsequent White House memorandum[25] tasked the DNI with establishment of a Cyber Threat Intelligence Integration Center to:

1. Provide integrated all-source analysis of intelligence related to foreign cyber threats,
2. Support Federal organizations addressing foreign intelligence threats,
3. Oversee development of intelligence sharing capabilities,
4. Ensure downgrading of threat intelligence to effect distribution to US government and private institutions, and
5. Facilitate and support interagency efforts to counter foreign intelligence threats to the nation.

The DNI is tasked with achieving full operational capability of the CTIIC by the end of fiscal year 2016.

***Comment: The Administration (and Congressional) emphasis on Privacy Protection and Information Sharing has very high priority but will make minimal contribution to protection of energy-critical infrastructure from cyber attack. Warning is not likely to be the issue; the nation has deep safeguards against surprise. And it is equally unlikely that improved flow of information from industry will do anything to correct the inherent insecurity of the Grid. Greater access to sensitive information on threats could of course, encourage industries to assume better defenses. But over-emphasis on sharing has left the Grid open to successful penetration by potential adversaries, Russia and China. The National Grid requires significant hardening; and that will only occur with leadership and cooperative action by Congress, DHS, DOE, DOD and the DNI, plus a significant change in priorities in the industry.***

## *B Department of Homeland Security*

By law and by Executive Orders, DHS has the primary responsibility for critical infrastructure protection for the nation's civil sectors. Its tools include a major cybersecurity staff, an intelligence organization that maintains knowledge of foreign threats, a 24/7 National Coordination Center linked to other federal organizations 24/7 watch centers, 16 separate industry Information security centers (ISACs) including the Energy ISAC at NERC. Additionally, US CERT is now subordinate to DHS and

[24] IAW EO 13549 Aug 18 2010 Classified National Security Intelligence Programs for State, Local, Tribal and Private Sector Entities and EO 12829 of Jan 6, 1993, National Industrial Security Program

[25] See Presidential Memorandum "Establishment of the Cyber Threat Intelligence Integration Center" February 25, 2015

continues its strong efforts to maintain detailed knowledge of active cyber threats and vulnerabilities of commercial systems. It remains to be seen if the new Presidential Executive Order on ISAOs adds significantly to the DHS tool set for Critical Infrastructure Protection.

The DHS has extensive responsibilities under Presidential Executive Order 13636 of 12 February 2013. The Secretary is responsible for an expanded classified and unclassified information sharing effort with all sectors as the Executive Agent for the Classified National Security Information Program (Sec 4), for protection of privacy and civil liberties (Sec. 5), for establishing an extensive program under the Critical Infrastructure Advisory Council with Sector Coordination Councils, owners, operators of critical infrastructure and sector-specific agencies of the government (Sec 6). The Secretary was tasked to establish and coordinate, within 120 days of the promulgation of the Framework, a program of incentives for private sector adoption (Sec.8d). Significantly, the Secretary was charged with providing the President the identification of critical infrastructure components at ***"greatest risk of catastrophic regional or national effects"*** including providing the President with annual updates and with notifying affected firms on a confidential basis (Sec. 9). The Secretary was also charged with taking NIST Framework "adoption steps' in conjunction with federal agencies.

***Comment: Keeping in mind that Presidential Executive Orders are binding only on federal agencies, the clear direction to DHS is to aggressively lead on the many provisions of EO 13636 relative to the private sector, enlisting the aid of any federal sector-specific agency. Regrettably, there is little evidence in the public domain of DHS taking a strong position on much of the above. There is, for example, no trace of DHS engaged directly with NERC or FERC on CIP v5, no trace of DHS direct involvement with the Energy sector on adoption of the NIST Framework, and Information sharing remains largely stalled, notably for Congressional reasons. Incredibly, DHS has taken no action to deal with foreign adversaries proven to be in Grid networks. On the contrary, DHS espouses a philosophy of "Trust DHS" knowing full well that it does not possess the capabilities to defend the nation's Critical Infrastructure. And there is no sign that DHS has identified to the President, the risks inherent in the enormous vulnerabilities of the Energy Sector spelled out earlier in this paper. There are no follow-on actions (in the public domain} to mitigate such risks, as called for in the EO. DHS may aspire to the trust of industry but it is rapidly losing the trust of National Security Communities.***

The recent White House memorandum tasks the DNI with establishing the Cyber Threat Intelligence Integration Center by 30 September 2016. Included in its responsibilities "ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible ", for distribution to US private sector entities as called for in EO 13636. Although the DHS is not an intelligence collection agency, this places significant additional responsibilities on DHS to directly engage with private sector entities to use such federal intelligence flows to ensure a reverse flow of threat information from the private sector.

*Comment: The issues on exchange of threat information are much more complicated than the White House memorandum or DHS emphasis would indicate. It remains to be seen if the security industry voluntarily shares its client-based most substantive threat studies with the NCIIC. The security industry is very competitive and there is also increasing evidence that US firms are extremely nervous about obligations to their foreign clients and dubious that foreign security firms are unbiased with respect to their foreign governments. This is a minefield and hard legislation will most certainly be required. Without clear liability protection under the law and considerable tutoring of privacy advocates, including those in DHS and Congress, such legislation will not be readily forthcoming. DHS is espousing the principal of "Trust DHS". But to what end? Precisely what is DHS's "Value Added"? It has shown no positive contributions to Critical Infrastructure Protection for the National Grid and worse, taken no steps to offset the penetration of the Grid by foreign adversaries. DHS has but one hope; that there will never be a major attack on US Critical Infrastructure. It has shown no leadership in developing an effective National strategy for Critical Infrastructure Protection. It has not the means to defend the US, even with industry's help. And it cannot engage in Active Defense of any Critical Infrastructure; that should always be the role of the National Security communities. It would be well-advised to strongly support this partnership and cut out the nonsense of "Trust DHS".*

## C. Department of Energy

DOE is a sector-specific department. It has profound responsibilities in both weaponry and energy nuclear fields; it is recognized as the major federal organization responsible for energy science, nuclear reactor research and of course, Green energy. DOE supports a national array of government-owned, contractor-operated laboratories, most recognized as world-class facilities. Maintenance of the nation's nuclear weapons stockpile is the primary role of DOE's semi-autonomous National Nuclear Systems Agency but DOE's primary role is Energy. DOE laboratories engage in a wide variety of security-related research tasks, some funded by other federal elements, the goals generally being longer-range deeply technical studies.

Doe Headquarters' Office of Electricity Delivery and Energy Reliability (OER) has the primary responsibility for support of Energy Sector cybersecurity programs. This Office is the major Energy policy organization in DOE and should be the principal threat vs. vulnerability advisory body within DOE and to FERC (and NERC.) As a federal sector-specific organization, DOE/OER is responsible under EO 13636 to work cooperatively (and voluntarily) with the electric utility industry. For example, DOE is tasked with extending the NIST Cybersecurity Framework into implementation. Over the past several

years, DOE has developed or identified a number of major tools to create what should be a highly cyber-secure national electric grid; specifically:

1. The Electricity Subsector Risk Management Process Guideline, 2012[26]
2. Guidelines for Smart Grid Cyber Security, IR 7628, 2010[27]
3. NERC's Critical Infrastructure Protection (CIP) Standards v3 (v5 by 2017)[28]
4. Cybersecurity Capability Maturity Model (C2M2) 2014[29]
5. Energy Sector Cybersecurity Framework Implementation Guidance, Jan. 2015[30]

***Comment: How well is this voluntary industry-federal partnership working relative to threats and vulnerabilities? The short answer is: not well at all. DOE/OER should be the main linkage on Grid threats between DOE's Office of Intelligence and the industry but has not filled this void. Further, DOE/OER's efforts to provide tools to the industry, described above, carefully circumscribe deeply technical Grid issues. DOE/OER is well-aware that the extensive linkages in the C2M2 Model to NIST standards (NIST SP 800-53 v4) are unacceptable to NERC, it is well-aware that NERC (and FERC) completely ignore EO 13636 Cybersecurity Framework imperatives, DOE/OER assiduously avoids references to the serious Grid vulnerabilities outlined in this (and earlier) papers. And while DOE deserves very high marks for its contribution to the SynchroPhasor/PMU initiative outlined earlier in this paper, its failure to mandate encryption of the SynchroPhasor program's network and communications components is inexcusable. In its support efforts for the Electric Industry, the Department of Energy is seriously failing in its broader responsibilities to the nation's security.***

## *D. Nuclear Regulatory Commission*

It is very important to get the NRC into context with other major topics of this paper. Earlier publications have dwelt extensively on the major vulnerabilities of nuclear sites, particularly site weaknesses brought to light by the Japanese Fukashima-Dai'chi disaster.[31] The NRC has worked very hard to establish an effective cybersecurity regulatory regime for nuclear generation sites, despite

---

[26] available at:
***http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20 May%202012.pdf.***

[27] available at:
***http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf***

[28] CIP V5 Transition guidance available at
http://www.nerc.com/pa/CI/Documents/V3V5%20Transition%20Guidance%20FINAL.pdf;

[29] Available at: ***http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.***

[30] *Available at:*
***http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.***

[31] See SECY-12-0095, NRC Policy Issue Information, On Tier 3 Lessons Learned report, July 13 2012

pressure from the industry to weaken implementation, mainly to conform to the much weaker non-nuclear industry standards being implemented under FERC/NERC oversight. The trade association Nuclear Energy Institute (NEI) has a petition pending before the NRC to do precisely that.[32]

The NRC cybersecurity regulations are tied into overall nuclear safety regulatory structures.[33] This ensures that site security plans and implementations directly link cyber systems to nuclear safety and security systems. Plant inspections will look for these relationships and any violations will be considered in the same light as those involving nuclear physical facilities. That's the good news.

The not-so-good news is that the site plans called for have been significantly delayed for several reasons; requirements clarification, differences among sites, shortage of cybersecurity expertise in inspection staff, and just the chore of working with over fifty different sites. Nevertheless, the NRC has not yielded on the technical depth of site cybersecurity defenses or their linkages to nuclear systems. There are, site by site, schedules for review of these plans to be completed by 2017. Thereafter, site inspections will review cybersecurity implementations as well as the normal nuclear security and safety systems. How critical are these plans? One only has to look at the aftermath of the Fukashima-Dai'chi nuclear crisis to see the effect of loss of off-site power following the tsunami:

**Fukashima-Dai'chi Nuclear Plant Site**

Nuclear contaminated ground water is collected and stored to prevent its flow into the Pacific. Long range plans call for inserting a deep refrigerated, frozen ground barrier to divert ground table water around the four buildings housing fractured reactor components and spent fuel pond

[32] NRC Docket 2014-0165-0001 "NEI Petition to Amend 10 CFR 73-54 "Protection of Digital Computer and Communications Systems and Networks" June 12, 2014

[33] NRC 10 CFR 73-54 "Protection of Digital Computer and Communications Systems and Networks", September2011

contaminants seeping into the ground. The stored water will eventually have to be filtered to remove contaminants. This is a further complication to the wide-area airborne contamination from faulty venting of damaged reactors, (a lesson the NRC has not fully absorbed.)

***Comment: The energy industry at large, and its nuclear component represented by the NEI have seized on the NRC delay to argue for reduction of requirements to that set of cyber assets indirectly coupled to nuclear systems, i.e., communications, maintenance, security management, etc. However, such cyber vectors must remain secure since they are logical pathways for indirect but sophisticated attacks on reactor and spent fuel vulnerabilities. The lessons of Stuxnet should not be forgotten; any cyberattack on a nuclear site by an adversary nation/state is bound to be highly complex. It is reasonable for the NRC to prioritize vulnerabilities and risks, and their strategy to rank these roughly against their four-tier physical security model is smart, but adoption of the vaporous CIP v5 standards at NRC sites should continue to be resisted.***

***Updating the agreement between FERC and the NRC on off-site power dependencies has been hung up for years because their regulatory independencies create a legal gap between the sources of off-site power, and the nuclear sites. Contract law applies, check the MISO RC web site for evidence. This can only be fixed by Congressional legislation; one of the several liability issues involving security in the North American Grid. The NRC must keep independent pressure of nuclear site vendors to ensure off-site power availability through stringent attention to communications reliability, despite NEI's efforts to eliminate the responsibility "at the first intertie". The preferred solution includes encryption of all such inter-site networks and communications systems.***

## *E. Congress*

In December 2014, the Congress sent five cybersecurity bills to the President for signature[34]. However, this legislation does not significantly affect the issues discussed in this White Paper. HR 2419 Comprehensive Information Sharing and Privacy Act has been reintroduced in the House but it has not yet been passed and sent to the Senate; proponents may be more successful in the new Congress in 2015 and if so, a Presidential signature may be contingent on upgrading the Privacy provisions of the Bill. Linkage of CISPA to the re-authorization of the Patriot Act could also occur since there is a small but vocal congressional caucus concerned with privacy issues central to both pieces of legislation.

There is much bipartisan support for other cybersecurity legislation, particularly In light of the Sony attack by North Korea, but it is doubtful that much will move until after months of hearings on a

[34]Gov Info Security "Obama Signs 5 Cybersecurity Bills", December 18, 2014

variety of cybersecurity topics. White House legislative proposals arising out of the Sony attack focus mostly on privacy and intellectual property matters. The Senate Select Committee on Intelligence has voted out a Bill centered on information sharing but also including some liability and privacy provisions. The Senate Homeland Security and Government Affairs Committee has initiated discussions with industry and privacy groups soliciting input for legislation[i] expected to be heavily focused on information sharing, liability protection and privacy matters.

***Comment: While the Information Sharing and Privacy issues will undoubtedly continue to dominate Congressional (and Administration) action, the major issues discussed in this White Paper require legislation, some urgently; notably the standards-only limits of the FPA of 2005, the liability issues inherent in private sector cybersecurity protection, the regulatory overlaps and disconnects between FERC and the NRC, clarification of department/agency responsibilities for combating malware and attacks, expanded missions for national guard units, and funding issues related to all of the foregoing. The burden on Congress will be to correctly balance energy industry interests with the greater interests of the public and the nation.***

## *VII. Grid Threats*

Threats to the Grid continue to increase, in magnitude and sophistication. While there are Intellectual Property (IP) objectives (sensitive technology, market control, etc.), most threats to the Grid are centered on development of attacks designed to take down electric generation, transmission or distribution systems. It is now clear that foreign adversaries have penetrated Grid networks (details below), undetected of course by Grid operators and the NERC CIP Standards process. It is instructive to understand the sequence of steps generally taken; a competent adversary would attack the problem as follows:

1. Open Source Collection of Grid details
2. Grid Reconnaissance, i.e., Topology, Security, Technology
3. Data/Information Extraction from the Grid
4. Vulnerability Assessments (Incl. Supply Chain)
5. Attack Development; Modeling & Simulation
6. Grid Resource Acquisition (e.g. Botnets)
7. Malware Insertion; Maintenance, Updates
8. Attack Testing (Covert, Anonymity, Deception techniques)
9. Parallel Intelligence Operations in Support
10. Training of Information Operation Cadres (Continuing)

## A. Nation/States.

Many countries have developed operational information warfare programs; the modern addition to their national security capabilities. Critical infrastructures of potential adversaries will be a major target objective but the difficulties of target knowledge, national priorities, trained manpower, target accesses, anonymity protection and fear of retaliation complicates attack development. However, much of what needs to be known is publicly available; certainly this is the case for the US National Grid. Reconnaissance will certainly be conducted to fill in the gaps.

Information Operations are now routinely used in armed clashes in troubled world areas[35] since most central governments are under substantial pressure from their Armed Forces to support the development of "Cyber Warfare" capabilities. Development is one thing, however use of those capabilities is another; it has quickly become a major national policy question and "deterrence" has become an important topic in overall national cybersecurity policy debates. The recent reports of Chinese and Russian malware in the US National Grid reflects policy decisions by those nations to conduct intelligence collection, reconnaissance operations and attack development against the United States in the critical area of Energy Infrastructure.[36]

### 1. Russia.

The Russian capability to conduct cyber operations against its adversaries has been demonstrated to the world in the Russia campaigns against Georgia, Estonia and more recently, the Ukraine.[37] And Cyber operations against the U.S. date back to at least 2007[38]. Security researchers describe these efforts as increasingly sophisticated and adroitly managed and a significant effort is underway in the security industry to plumb the depths of Russian malware. According to the antivirus firm Kapersky Labs, for the past two years, a Russian group that has built its malware around a tool, labelled "BlackEnergy" that has upped use against the National Grid[39]:

***"The group seems particularly interested in targeting organizations that run industrial control systems, especially from the energy sector. Victims identified by Kaspersky include power generation operators, power facilities construction companies, suppliers and manufacturers of heavy power-related materials, and energy sector investors."***

In one case, attackers downloaded and executed a BlackEnergy plug-in called "dstr" that destroyed data on an organization's Windows computers. This plugin is designed to obscure traces of BlackEnergy when control over the victim is lost. US CERT notes that the Kapersky findings are consistent with other reporting that confirms that vendors of human-machine-interfaces (HMIs), such as General Electric, Siemens and BroadWin/Advantech, had their systems infected with BlackEnergy-

---

[35] Reuters "Security Services Foiled Massive Cyber-Attack on Israel" August 28, 2014

[36] US CERT, (ICS-ALERT-14-281-01A) "Ongoing Sophisticated Malware Campaign Compromising ICS (Update A)" October 29, 2014

[37] Reuters "Cyber Snake Plagues Ukraine networks" March 7, 2014

[38] Novetta SMN op.cit.

[39] IDG News Service BlackEnergy Cyberespionage group targets Linux systems and Cisco routers" 4 November 2014

associated malware. These supply chain penetrations of course result in inadvertent downloading of the malware when upgrades are loaded. HMIs are software applications that provide a graphical user interface for monitoring and interacting with industrial control systems. The Grids' increasing reliance on PMU data for its human controllers may well be the intended purpose of these Russian intrusions.[40]

***Comment: It is truly astounding that these aggressive cyber operations, underway for the past several years, have had no effect on the development of effective CIP standards, or to provoke the encryption of PMU data. NERC and FERC continue with the fiction that those standards, with unsupported claims of Grid resiliency, are sufficient to maintain the survivability of the Grid. Industry "complacency" (to be kind) points to the absence of an identified successful cyber attack as evidence it can't be done. The overwhelming evidence from security analysts is that the malware now being seen (in combination with sophisticated command and control strategies which they can't observe) is more than capable of serious Grid disruption. What is even more astounding is that National leadership, the Congress, the White House, federal agencies with responsibilities for national security and the protection of Critical Infrastructure (DHS, DOE, DoD, DNI, etc.), would passively accept the NERC/FERC strategy, documented in this White Paper, given their knowledge of the threat. These are not threats to intellectual property but efforts that have as their purpose, taking control over critical infrastructure or destroying it.***

## 2. China


Much has been written on the long history of Chinese cyber attacks on US institutions. Most can be characterized as industrial espionage; theft of information and data extremely useful to Chinese industry, including Defense Industry. A former ex-Director CIA labeled such efforts as the greatest transfer of wealth in history. Almost no American institution has been immune; the list of Chinese property thefts includes scientific, industry, government, financial, health, social, academic topics. And for sophisticated access, this has included zero day attacks, cryptographic certificates, password files and the like. Chinese-developed malware exists in depth or is purchased on the open market. Most of these efforts have been identified through US government forensic programs and increasingly from deep studies by the U.S. security industry.

China has a history of cyber operations to control dissent in its homeland. And the central government has strong influence over its IT industry such that Chinese services and products are treated

[40] See North American Synchrophasor Initiative (NASPI) "Technical Workshop, Phasor Tools Visualization" June 13, 2012

with considerable suspicion abroad. A recent report on major flaws in over 700,000 routers supplied to clients by ISPs is a case in point[41]. The suspect routers are almost entirely using "flawed" firmware provided by a single Chinese company and coincidentally, the majority of attacks on these routers are from Chinese IPs. This is almost certainly a world-wide sophisticated supply chain attack.

A deep study of a Peoples Liberation Army unit 61398 located in Gaoqiaozhen, near Shanghai, has revealed a great deal of information on this Chinese threat actor, one of more than 20 Chinese cyber activities identified in this study.[42] This unit is a part of the PLA's signals Intelligence effort and appears to be well-supported by associated captive laboratories. Additionally, China Telecom has provided wideband fiber optic connectivity to support its CNE function. Operators are proficient in the English language, knowledge of many Information Technology products and systems, and computer skills. Nearly 100 % of the remote clients (IP addresses) used to infiltrate their targets are registered in China. The size of the collection effort implies a very large organization to maintain mission and targeting knowledge, intelligence requirements, linguistic resources, training, analysis and reporting. These incursions have become so blatant that the US Department of Justice has indicted five individuals associated with PLA Unit 61398.

It is not the intention of this paper to detail the infrastructure, command and control, tools and techniques used by this Chinese PLA unit. The referenced Mandiant APT1 report is very detailed on these topics. The important question is: What is the mission of this unit relative to Security of the North American Grid? Targeting shows interest in the energy industry and in SCADA technology but this is consistent with its broad espionage effort. ***There is no direct evidence of a mission of this unit to attack the Grid.***

Nonetheless, Admiral Mike Rogers, Director NSA/Commander US Cyber Command, on Nov 20, 2014 before the House Intelligence Committee stated:[43] **"There are multiple nation-states that have the capability and have been on the [industrial] systems. We see them attempting to do reconnaissance on our systems"** to steal **"specific schematics of most of our control systems down to the engineering details."** In the past, U.S. intelligence officials warned that the Chinese had penetrated the electric grid. Rogers confirmed that **"there's probably one or two others"** that have also wormed their way in. **"There shouldn't be any doubt in our minds that there are nation-states and groups out there that have the capability . . . to shut down, forestall our ability to operate our basic infrastructure, whether it's generating power across this nation, whether it's moving water and fuel."**

Well, if it isn't the PLA, where's the smoking gun? A good bet would be Axiom, a Chinese CNO organization that has been the subject of deep study by a consortium of Security firms.[44] Axiom is the most sophisticated Chinese cyber attack organization, apparently outclassing PLA Unit 61398 in scope, competency, operational security, persistence on target, and sophistication of attack strategy. Its targets are global, diplomatic, industry-selective, NGOs; i.e., clearly strategic in nature. Its multi-tier attack strategy is complex involving target identification, reconnaissance, penetration, horizontal

---

[41] IDG News Service, "At least 700,000 routers given to customers by ISPs are vulnerable to hacking" March 10,2015

[42] Mandiant APT1 Report, "Exposing One of China's Cyber Espionage Units", 2014

[43] National Security Agency "Comments of Adm. Mike Rogers before House Permanent Select Committee on Intelligence, November 20, 2014

[44] IBTimes "China-backed hacking group Axiom said to have attacked 43,000 Computers" February 8, 2015

exploration, infrastructure creation and control, malware customization to target, and attack profile management, to avoid detection. Energy organizations are an identified major target for Axiom. The organization is characterized by extreme care in its operations, not a single Axiom compromise has been observed, as have been seen for PLA Unit 61398,[45] Axiom clearly serves the strategic interests of the Chinese government and would certainly have a major role in planning for a takedown of the US Energy Grid.

## *B. Rogue States.*

Another class of countries represent somewhat different threats to critical infrastructures, less an adjunct to military action and more an effort to use the asymmetrical power of cyber attacks in retaliation for a grievance against another country. Examples include the Syrian Electronic Army persistent attacks on the US; Iranian attack on Saudi Oil and Gas production, North Korean attack on Sony in protest for the disparaging film on North Korean leadership.[46] Rogue states can be leveraged into action by other states that wish to remain anonymous. As with larger nation/states, these second and third tier countries are capable of developing or buying sophisticated attacks and using them when their leadership demands it. With easy access to US networks across the WEB, Rogue states are no longer limited by physical access to nations they wish to attack. Taking control of US systems, often without the user being aware, provides the base for their incursions. The Grid itself is wide open to establishing the Botnets that would be used in many attacks, DDOS as well as more sophisticated malware. They would hardly be troubled by the weak CIP v5 standards.

### *1. Syria*

The Syrian Electronic Army, an adjunct to the Assad Regime, is a loosely-knit ideological organization that has attacked many western institutions which they consider anti-regime. It operates rather openly and is therefore fairly well-understood by security analysts. It is capable of a number of attacks, including spear-phishing, Web site defacement using SQL injection, DNS hijacking, fabricating Facebook and YouTube sites to collect log-in credentials and spread malware, and disseminating DDoS attack tools. It has targeted media web sites and last Thanksgiving succeeded in getting pop-up ads on a number of websites, like NBC, Forbes, The Chicago Tribune, NHL, The Telegraph, using GoDaddy to alter the Domain Name System for Gigya to get to the sites and place their messages. ***There is no evidence that the SEA has targeted the Grid or has developed the tools to do so***. However, there are recent NY Times reports of a successful Assad regime cyber attack on insurgents leading to significant insights to insurgents' tactics, logistics and other tactical data. It is not known at present if these operations were conducted by SEA or by another Syrian cyber warfare group.

---

[45] Novetta Operation SMN: "Axiom Threat Actor Group Report", 2015

[46] Many accounts cast doubt on the certainty that it was North Korea; however the FBI asserted that forensics left no doubt about the attacker.

### *2. Iran*

Iran has been involved in cyber activities for a decade. It has a well-educated population, is technically mature, is surrounded by states it has opposed, aspires to nuclear statehood, and has been cyberattacked at the highest levels of sophistication. It has been characterized, perhaps excessively, as "the new China" in cyber warfare.[47] Rudely awakened by Stuxnet, in 2013 Iran mounted a Shamoon cyber attack on Aramco, Saudi Arabia's national oil company and one of the world's largest producers. The intruders wiped data from office computers, but failed to reach production systems, which were the main target. The Aramco attack failed because the company had one network for its administrative offices and a separate one for its production facilities. The attack nonetheless cost the Saudis considerable resources and embarrassment.

According to the referenced report, the Iranian cyber warfare structure is obscure but apparently includes private firms and Iranian hackers, but with fairly strong control by Iranian intelligence authorities. They are secretive and maintain good operational security over these efforts. Since Stuxnet, a number of Iranian operations have been unearthed by various security firms, including debilitating attacks on US banks in 2012 and 2013, and on the NMCI (US Navy-Marine Corps Internet). In February 2013, Israeli Prime Minister Netanyahu accused Iran of massive ***"non-stop" attacks on [Israel's] vital national systems"*** including ***"water, power and banking"***.[48] Iran was an active participant in the global campaign against Israel during the recent Gaza campaign.

In 2011, Iran was the source of the major attacks on the Netherlands Certificate Authority (CA) firm, DigiNotar. Earlier in 2011, another (Italian) CA firm, Comodo had also been hacked. It was months before authorities could determine the full extent of these hacks and trace them, circumstantially, to Iran. The theft of these certificates may have been linked to an internal Iranian campaign against suspected Iranian dissidents. Eventually Dutch authorities (as a user of DigiNotar certificates) had to advise Dutch citizens to avoid computer use in communicating with national agencies.[49]

Following the attack on Israel associated with the Gaza campaign, Israel announced intention to further protect critical infrastructure. Could Iran mount an attack on the US Grid? It certainly could develop the capability if it had not already. Understanding the vulnerabilities of the US Grid would be a prerequisite. Is this likely to happen? The answer is buried in a sea of uncertainty involving US-Iranian nuclear negotiations, related sanctions, pre-occupation with a myriad of regional conflicts, most obviously demanding of cyber warfare resources, and of course one of the major lessons of Stuxnet.....***Deterrence*** ....don't underestimate the big boys.

---

[47] Cylance, "Operation Cleaver Report", 2014

[48] The Hill "Israel, Iran Locked in Escalating Cyber War" 4 March 2015

[49] IEEE Spectrum "DigiNotar Certificate Authority Breach Crashes EGovernment in Netherlands", September 9, 2011

## *C. Hactivists, International Criminal Elements, Cyberterrorists.*

These are probably the most likely elements to actually attack the Grid. Many classes of useful malware are on the market at fairly low prices, capable in the right hands of doing extensive damage; e.g., massive distributed denial of service (DDOS) attacks, ransomware packages capable of major blackmail attacks, leased botnets for capturing control of unprotected facilities, disinformation campaigns. It is well-established that Russian criminal elements act as surrogates for the Russian government; likely shielding the federal authorities from direct identification. The aforementioned attack on Israel included Anonymous, a worldwide Hactivist organization, essentially choosing up sides between Israel and Hamas. Anonymous has threatened the Hong Kong government and more recently is engaged with other activists in challenging ISIS on Facebook. Anonymous is, as expected, experiencing a schism as its elements align with regional social and political imperatives. However Anonymous fractures, ***the only thing required with this group (or groups) is a "cause"***.

There has been much concern expressed over the possibility of international terrorists attacking the US critical infrastructure. While there is no direct evidence of an immediate threat, this is precisely the type of retribution the US can expect when (not "if") terrorist organizations eventually develop the expertise to mount serious attacks. The Grid is an obvious major target, as are US nuclear sites, since widespread casualties would be the major purpose for such attacks. With the emergence of ISIS from the Syrian insurgency, there is frequent speculation of a near-term ISIS assault on US critical infrastructure. However, while the ISIS motivation for this is clear, much has to occur within ISIS before any reasonably sophisticated attack on the US Grid will occur.

However, an "international' Islamic threat is emerging in the organization known as the Cyber Fighters of Izz ad-Din al-Qassam. In 2013 this group launched distributed denial of service (DDoS) attacks against the websites of a number of banks and credit unions. The group generally uses compromised servers in hosting companies that are often located in the U.S. The Cyber Fighters claim the attacks will continue until YouTube removes an anti-Islam video that mocked the Prophet Muhammad. Iran denied any involvement.[50]

During 2014, many of the nation's largest banks have been pummeled by massive distributed denial of service (DDoS) attacks. The attacks have been notable because of their sophistication and persistence. Security firms which specialize in helping companies mitigate DDoS attempts, have noted how some attacks generated magnitudes more DDoS traffic than anything seen before.[51] The attacks ceased during the Iranian elections; essentially confirming that they are being orchestrated from Iran. Izz ad-Din al-Qassam Cyber Fighter has claimed responsibility for some of the early attacks, but security experts feel certain that others are involved as well. . Some analysts are associating this group with the Iranian government's attack against dissidents. In the past few years, the Iranians have acquired or nationalized telecoms, established filters, cutoff switches for the Internet and infiltrated Facebook, Twitter, YouTube. Iran has established a high degree of surveillance and control. Coincident with the

[50] Computerworld, "Quantum Dawn 2 will test Wall Street Cyber Readiness" July 17, 2013
[51] CSO, "Islamic group promises to resume US Bank cyberattacks" 28 February 2013

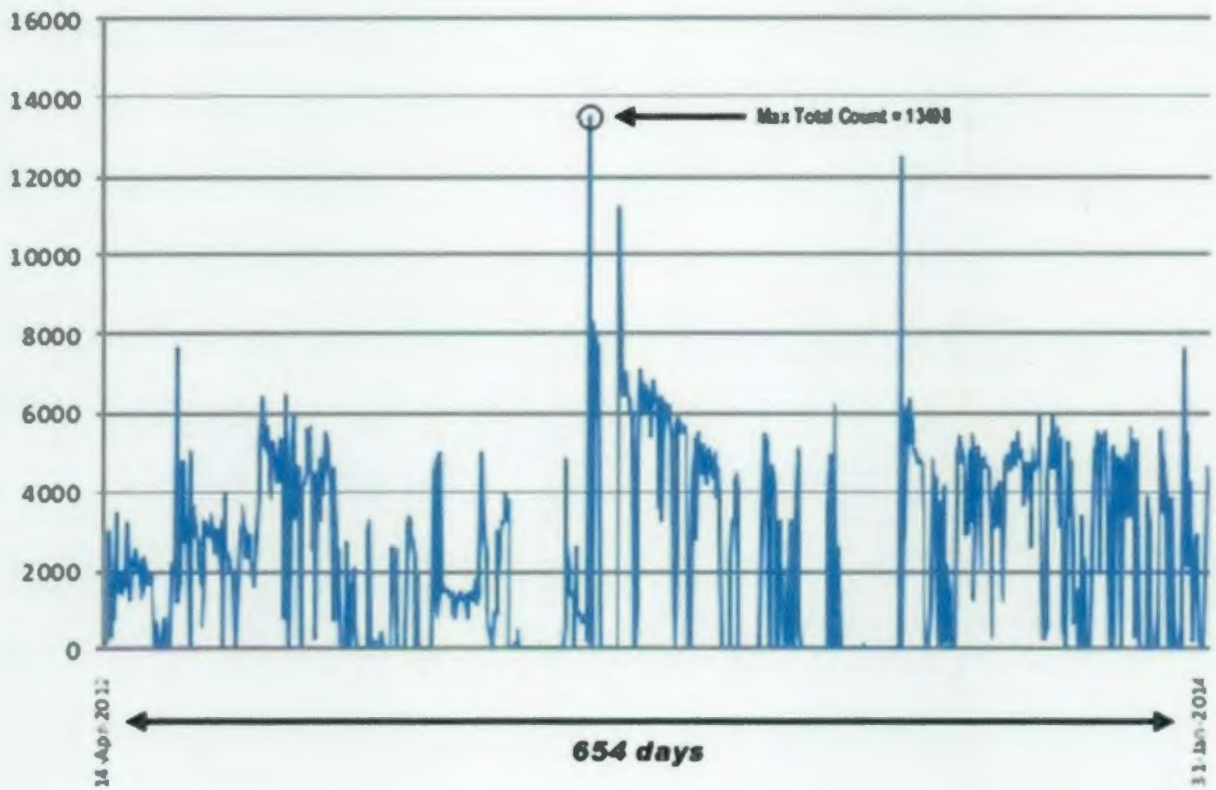
Iranian elections, a major phishing campaign was orchestrated, apparently to influence the outcome of the election. The growth of these ideologically-motivated attacks is further evidence of the growth in Iran's ability to muster a broader segment of hactivists' Islamic support.

## *VIII. Vulnerabilities*

### *A. Industrial Control Systems, Programmable Logic Devices*

Modernization of the Grid over the past six decades has led to automation of switching and control systems. The generic term, programmable logic controller, as the name implies, covers industrial control systems (ICS) that can be programmed to perform multiple functions. ICS have not been designed to be secure and, they are often remotely managed and are in the direct link for Grid operation. How bad is the exposure of ICS devices to Web access? Very bad. A recent article[52] involving the SHODAN mapping system revealed an average of over 3000 devices per day. Over the period of the study, over 2.8m unique IP addresses were logged. Hundreds of thousands of these devices represent the major vulnerability of the Grid, an almost impossible security challenge for the industry. Since it will be decades before these devices will incorporate security features, the only possible security fix requires restriction of these devices to dedicated encrypted networks. This vulnerability alone emphasizes the degree to which the CIP v5 Standards miss the mark.

***SHODAN Count of WEB-accessible ICS-related Devices April 2012 to January 2014***




[52] IEEE Spectrum, "Internet-Exposed Energy Control Systems Abound" October 21, 2014

This vulnerability is seldom discussed by the industry and has been nimbly avoided by NERC (and FERC) over the history of critical infrastructure developments. Not so by US CERT who routinely publicizes this vulnerability in its work. The STUXNET attack on Iranian centrifuges was a remote application of PLC disruption causing serious damage to Iranian nuclear programs. One of the lessons from that attack is that a very sophisticated program of disruption can confuse and mislead facilities management over an extended period, before the "attack" is realized.

One such theoretical attack has been shown in a vulnerability experiment titled Aurora, tested at the DOE Idaho National Lab. It has been theorized that it was possible to destroy many mechanical system (motors, pumps, cooling systems, etc.) by deftly and rapidly switching such systems off and on. For safety and reliability purposes, such devices are often protected by relays; however, remote mistreatment can cause these relays to fail. The Aurora experiments demonstrated precisely this. Note that Industry savants state that Aurora's complexity coupled to the inherent resiliency of the Grid make this a highly unlikely attack.[53] However, Stuxnet is an actual benchmark for remoted attacks.

## *B. SCADA/EMS systems*

One level up from PLCs are SCADA systems, Supervisory Control and Data Acquisition Systems, a nominal feed to Energy Management Systems (EMS). Such systems are often very complex, computer controlled, accumulating and tabulating digital data from ICS/PLCs and providing the interface, i.e., the controlling system for remote management. Only a handful of international companies produce SCADA/EMS systems and most designs preceded cybersecurity programs. Exploiting SCADA vulnerabilities was, in fact, part of the attack strategy for STUXNET, and these have subsequently been extensively studied by security experts. It will be many years before deployed SCADA/EMS systems can be replaced by more secure systems; hence they will continue to represent a major unsecured vulnerability of the Grid. Here again, the NERC/FERC cybersecurity standards carefully avoid explicit identification of this vulnerability, it does not show up in any of the requirements underpinning the CIP v5 Standards, nor is it the subject of any significant discussion in the multitude of formal exchanges of the CIP process.

**Comment: The general public cannot appreciate the complexity, and therefore the uncertainty, of the security interrelationships of transmission and distribution systems at a local level. While the local utility firm will undoubtedly bill users for power consumed, the user may not know that their power comes from a regional consortium of utility firms whose liability is uncertain. Individual members of the consortium, satisfying the minimum requirements of CIP v5, might be held accountable for their contributory activities, but there does not appear to be any overall joint accountability. And their local utility, "a distribution entity" may be exempt from the law. NERC and FERC talk excessively about "responsible entities" but exactly who is the "responsible entity" at the intersection of the BES and the "distribution" system" relative to security protection? The virtualization of the Grid, its transmission and distribution systems, seriously obscures responsibility for security. Contract law is likely to apply in any legal liability action since the FPA fails to adequately cover the entire Grid.**

[53] Defense One, "A Hacker's Hit List of American Infrastructure" January 2, 2015

The recent (April 7, 2015) DC/Maryland area power outage illustrates the confusion of responsibilities that would also be experienced in a wider-scale cyber attack. The cause was a pylon failure in southern MD, causing the loss of a 235 Kva line. PJM, a not-for-profit utility (that also doubles as the Reliability Coordinator for DC and 13 states) controls area wide transmission services. PepCo utility is a member of this consortium, however the original line loss took down two power stations run by SMECO, a regional distribution cooperative as well as two other key PepCo's connection points.[54] PJM had overall management of the outage with cascading instabilities that ultimately affected the Calvert Cliffs nuclear facility in Maryland,[55] dependent on off-site power for cooling of its twin reactors. This caused both reactors to shut down with a combined loss of 1829 MW to the area. An event report was filed with the NRC.[56] One back-up diesel generator failed to start but the emergency backup was implemented so reactor cooling was not adversely affected. Fortunately, PJM was able to adjust overall power from the Grid into the DC/MD area to compensate for the loss of Calvert Cliffs; had it been at either Summer or Winter peak loads, the outage would have lasted longer, according to industry experts.

**Setting aside the understatements of PJM and PepCo, *the initial failure was below the FPA 2005 thresholds set for Critical Infrastructure Protection. Had the overall outage been caused by a cyber attack, what organization would have been responsible for addressing it? Where is Grid-wide operational cyber security vested? What needed to be centrally monitored to address the attack? What information flow should be active to support "situational awareness"? Had the attacker been orchestrating the attack, what would its reaction have been to the PJM adjustments? Could the presumed resiliency of the Grid been able to adjust? Or would it eventually lead to a nuclear crisis at Calvert Cliffs?***

## C. Communications and Networks

If ICS and SCADA/EMS systems are nearly totally vulnerable to remote attack, they should be completely protected by cryptographically-secure communications and network systems. The FPA 2005 unquestionably called for this. And after nine years FERC has ordered a "definition" of communications networks! CIP v5 Standards deliberately fence out Grid-wide communications and network systems, limiting security controls to facilities within defined site security perimeters. These vulnerabilities are further compounded by the industry practice of using its Internet connectivity for business, management, marketing as well as technical operations. There is no complete topological mapping of Grid-wide communications and networks; it is likely that this is now best understood by the nation's most advanced adversaries.

## D. Control Centers

Major utilities operate control centers to synchronize their generation, distribution and transmission efforts. These inevitably involve interconnections to other regional utilities, and with the BES, for coordination of power exchanges. The power exchanges are sensitive to technical requirements for frequency and current balancing purposes. Among the many responsibilities of control centers,

[54] Washington Post, "Power urge takes out electricity in parts of D. C. region", April 8 2015
[55] Bloomberg Business, "Washington Power Falls as Grid Adjusts to Power Failure, April 7 2015
[56] NRC Power Reactor Event Number 50961, Facility: Calvert Cliffs, April 7 2015

increases and decreases in power demand create a technical management responsibility for control centers which must manage "reactive" and other power resources to keep the BES "balanced". The long term integration of the Grid, expansion of interregional connectivity, the need for regional flexibility, and of course the unknowns of cybersecurity incidents have created need for automation of the Grid balancing function. The industry has incorporated several major technologies to address these needs; see for example the earlier discussion of SynchroPhasors and Solar DC/AC inverters. The security issue is how vulnerable are these newer technologies and importantly, their control center data management systems, to deliberate interference and manipulation?

## *E. Off-Site Power Transmission systems feeding Nuclear Sites*

One of the major safety strategies for US nuclear generation facilities is the requirement to provide ac power from off-site sources. The failure of off-site power delivery to Fukashima Dai'chi was the proximate cause for the multiple explosions and wide-area nuclear contamination, since reactors and spent fuel ponds could not be cooled. FERC/NERC and NRC agreements address the need for off-site ac power; however, the "agreement" at RC implementation levels is little more than paper. At present nuclear utilities must negotiate ac power contracts with generation or transmission owners and operators supplying such power. Recently, however, the Nuclear Energy Institute[57] petitioned the NRC to reduce site communications cybersecurity requirements to the first "intertie", this would essentially eliminate the "issue". The NEI effort is clearly an attempt to introduce narrowly-defined Perimeter Security (PSP) similar to the CIP v5 standards supported by FERC, but a clear violation of the FPA of 2005. If the NEI petition is accepted by the NRC, it will result in a major increase in the vulnerability of nuclear sites.

***Comment: Most government and university cybersecurity experts postulate a risk-management strategy; users must accept the reality of cyber penetration and must accept the need to manage risks. The NIST Framework is, in fact, a risk-management strategy. But is it possible to manage risk against complex threats (and contentious vulnerabilities) described at length above?***

***In 1921, a noted University of Chicago economist, Frank Wright, wrote a seminal paper that differentiated risk from uncertainty. Risk, he argued, is something that can be modeled and mathematically measured. Uncertainty is the deep unknown. His theory is a cornerstone of modern economics. In cybersecurity, if vulnerabilities are unclear or uncertain (as is the situation in the Grid), and "risk" cannot be modeled and measured, it cannot in any sense, be "managed." For deep and uncertain threats to the National Grid, a more pragmatic strategy is absolutely essential.***

[57] NRC Docket 2014-0165-0001 June 12, 2014 op.cit.

## F. Disaggregatioin of Electric Industry

Deregulation of the electric industry is a powerful roadblock to cooperative cyber defense; hence a major vulnerability. This is easily seen in the lengthy and yes, peculiar approach to setting CIP standards, extending to the regulatory agencies and significantly, to the federal institutions responsible for critical infrastructure protection.

> ***Comment: There is no major issue of survival of the national grid covered in these white papers that is not skewed by the singular determination of the industry to resist re-regulation, even when expert studies of threats and vulnerabilities show the extreme danger to the nation. The industry has withheld most evidence of reconnaissance of the Grid by potential adversaries; it has been left to the security industry and federal forensic experts to document these penetrations. What has become evident in the last few years is the extent of that penetration. Hence, the major challenge is not that an attack will be mounted against the Grid but that the industry and CIP oversight authorities continue to permit the development or refinement of attacks that, in the absence of change, will surely succeed.***

## G. What Organization is Responsible for Active Defense of the Grid?

The importance of the National Grid to the United States is without question. The entire country is dependent on the Grid for electric power; all elements of society, the economic system, the healthcare infrastructure, the entire national security community simply cannot function if electric power is lost. The energy industry has been singularly endowed by the FPA of 2005 with responsibility for ensuring the reliability and security of electric power for the nation. Yet, a decade later, that industry asks its users to accept its judgment that resiliency and self-developed and vacuous standards suffice to provide protection from sophisticated cyber attacks; that a Grid-wide operational cybersecurity program is not needed; that its massive digital control system cannot be subverted, that the entire communications and network infrastructure need not be secured.

The risks to the nation and its population are incalculable. It's well-known that the energy industry will default to the federal government for cyber defense, if and when the nation is attacked. But even a premier cyber defense organization (i.e., US Cyber Command) cannot instantly take on sophisticated adversaries that have had years to reconnoiter the Grid as a target, seize major network and control assets and prepare complex attack systems. Such is the status today, with the Russian "BlackEnergy" and an even more obscure Chinese cyber organization (Axiom) infecting the National Grid. A cold start against such adversaries will simply fail; a huge loss of life will occur.

And the DHS cannot perform the active defense function; it lacks competency but more importantly, it is outside the national security community charged with defense of the nation. This major policy issue is left in the wreckage of a fragmented critical infrastructure protection program, marching to the drumbeat of information sharing, privacy advocacy, and a security industry (and DHS) resisting the inevitable.

So in the face of an irresponsible electric industry and a captured regulatory commission that will not prepare for adequate cyber defense, what can the nation do for "***active defense***"? ***This paper proposes that the National Guard be authorized, trained and equipped to perform the active cyber defense function for the National Grid.*** The National Guard has historically been used in the Nation's defense during crises and critical infrastructure protection certainly qualifies as a modern mission for the Guard. This will take years of course but hopefully not as long as the decade wasted under the 2005 FPA. Computer-competent talent can be, should be recruited to perform this function; trained in-place on grid control systems, to assume the Cybersecurity defensive role in any national emergency. There have been several public statements on the need for the NG to be trained and used in Military Cyber operations; a role in Critical Infrastructure ***Active Defense*** has not been apparent. Legislation will most certainly be required (including amendments to the FPA) along with substantial cooperation of the Department of Defense in conjunction with the States to develop the budgets, framework, training and support for such a mission. DoD has a major command, NorthCom whose sole mission is defense of the North American continent, its military and critical civil institutions. Additionally, critical linkages to the U.S. Cyber Command and national intelligence services/agencies will be needed.

The National Guard itself would need to develop the state-by-state CIP organizations. Many states are already lost in the maelstrom of critical infrastructure policy so should welcome the role this paper advocates. In the event of warning or implementation of an actual attack, NG organizations will have to integrate to parallel the 16 regional reliability structures that, in peacetime, form the operational reliability structure of the Grid. A cadre to support a pilot cybersecurity effort in one of the eight Reliability Regions should be recruited from the multi-state National Guard, (the 14 state region encompassing the PJM transmission area, for example.) A critical feature of this initiative will be the installation of an Einstein 3 system at control centers for training and use by National Guard augmentees. Guard cybersecurity cadres should be cleared for access to threat information at the Secret level. Initial exposure to Grid control systems and cyber defense should occur in those regional control centers that have functional responsibility for reliability management of the Bulk Electric System (BES) and in those control centers affiliated with Distribution systems that exist outside the FPA.

The Air National Guard might similarly train for protection of the nation's Air Traffic Control networks.[58] The Coast Guard could similarly be structured to address cybersecurity protection to maritime ports and seaways. The requirements, vulnerabilities, cybersecurity gaps and threats lie outside this White Paper.

## *IX. Summary and Conclusions*

Eighteen years after PD 63, 12 years after the Eastern blackout of 2003, tem years after passage of the Federal Power Act, and two-to-three years before CIP Version 5 standards go into effect, and with adversaries' malware in the National Grid, the nation has little or no chance of withstanding a major cyber attack on the North American electrical system. Incredibly weak cybersecurity standards with a wide-open communications and network fabric virtually guarantees success to major nation states and

[58] See GAO 15-221 Jan 2015, "Information Security - FAA Needs to Address Weaknesses in Air Traffic Control System". The majority of recommendations were not released to the public.

competent hactivists. This industry is simply unrealistic in believing in the resiliency of this Grid subject to a sophisticated attack. ***When such an attack occurs, make no mistake, there will be major loss of life and serious crippling of National Security capabilities.*** In the absence of a credible national cybersecurity deterrence strategy, the question is "Can the national leadership and the Congress and the Industry collaborate on the following critical steps to effectively protect the National Grid?"

- This must be initiated with an emergency program to encrypt all communication networks used for control of power transmission systems; i.e., all communications linking Reliability Centers and Balancing Authorities, the flow of SynchroPhasor PMU data, SCADA/EMS control functions, and any network involved in off-site power flow and flow management to nuclear sites. The security architecture needed for this immediate program must be initiated under each of the Regional Reliability Coordinators, downward, to encompass all facilities described above. A task force comprising minimally DOE, FERC, NERC, NRC, NIST, DoD/NSA can survey Grid topology and lay our an architecture with recommendations for phasing and funding. Legislation may be necessary to ensure industry cooperation.

- ***The process of encryption must be preceded by guaranteed expunging of adversary's malware from the Grid using Red Teams under Federal control.*** The Regional Reliability Coordinators must be empowered to oversee these functions within each reliability region. The Task Force cited above, augmented by industry experts, could lay out the strategy for accomplishing this. Any legislation needed to accomplish this, including federal funding or rate/tariff adjustment authorities, must be addressed by Congress.

- In parallel with the foregoing, a Task Force should be established to recommend to the President, an overarching 24/7 ***operational*** cybersecurity architecture for the National Grid, including all electrical distribution elements excluded from the FPA of 2005, including Alaska and Hawaii. The Task Force should be led by DoE and must include DHS, DoD, DNI, NSA, NIST and NRC, with observers from FERC and NERC. Overall Task Force recommendations must be actionable under either a Presidential Executive Order or additional Congressional legislation.

- FERC must hold all outstanding actions on CIP standards in abeyance pending completion of the above.

- In parallel, the DNI should produce an NIE on current and projected threats to the National Grid. That NIE should be forwarded for action to the National Security Council for deliberations on a National Strategy for countering threats to National Security and Critical Infrastructures.

- /FERC must immediately amend its Order No 802 to include a requirement for physical security standards involving transmission, generator and related distribution facilities identified by DoD, the DNI, HHS, (and such other national authorities) that are deemed critical to survival of specific facilities of critical infrastructure. Nominations should be reviewed by the White House; the identification of sensitive facilities should be classified.

- The crisis roles of DOD (NSA allied with Cyber Command) must be unambiguously de-conflicted with those of DHS by the Administration relative to roles in ***active defense*** of critical infrastructure, in an Executive Order, (with classified annex). Legislation as required and amendment of existing Executive Orders should follow.

- In open recognition that cyber warfare should be conducted only by military forces, the Secretary of Defense should create a Task Force under Northern Command to develop a long-term program for use of the National Guard as an adjunct to US Cyber Command in a combat support role for ***active defense*** of the nation's Critical Infrastructures, initially focusing on the National Grid. (This NG role should be affirmed by the House and Senate Armed Services Committees.) State authorities will need to be engaged. For the National Grid, the organization and training of NG units must overlay the in-place Reliability Regional structures.

- DOE with DoD, DHS and the DNI should be tasked to develop for White House approval, proposed legislation to codify substantive revisions to federal cybersecurity laws to strengthen the authorities of FERC and the NRC for cybersecurity programs to correct current deficiencies, conflicts and overlaps, to ensure the creation of a durable 24/7 operational cybersecurity program for the Grid, and to establish the essential linkages between the civil sector, the national warning and intelligence services, and military forces capable of ***active defense*** of the Grid.

- A process must be developed for integrated decision-making for effectively responding to attacks on the National Grid; attacks defined as any penetration, preparation for information warfare, and beyond, comparable for what exists in military cyber environments. These procedures must be folded into the President's wartime powers authorities, by legislation.

- In a deep study such as this, it has become clear that the "Red Line" between US industry cybersecurity firms forensic efforts and critically-important US classified capabilities is being increasingly violated, compromising intelligence sources and methods but also endangering the nation's ability to effectively engage its foreign adversaries in cyber combat. The conflict between business practices and reasonable classification laws is overdue to be addressed as a matter of strategic national policy. The courts have consistently held the view that the federal government has the constitutional authority to enforce measures for protection of sensitive information. Firms that knowingly publish the technical details of suspected US classified cyber attacks or defenses should be subject to the espionage laws or when under contract to a foreign entity, be required to register as an agent of a foreign power. This is a serious issue, and admittedly one that would be stoutly resisted by industry, privacy and antiestablishment advocates, but it can no longer be swept under the rug. A national commission should be empanelled to address the issue. In the interim, the Justice Department should be called upon to investigate any egregious cases.

Mr. George Roland Cotter
193 Southdown Rd.
Edgewater, MD 21037

UNITED STATES POSTAL SERVICE
1000
20555

U.S. POSTAGE
PAID
EDGEWATER,MD
21037
APR 18, 15
AMOUNT
$2.66
00101117-05

FIRST CLASS

The Honorable Stephen G. Burns

Chairman, U.S. Nuclear Regulatory Commission

Washington, DC 20555-0001